

THE HONORABLE JAMES L. ROBERT

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

*In Re: Zillow Group, Inc. Session Replay
Software Litigation*

This Document Refers to: All Actions

Master File No. 2:22-cv-01282-JLR

MICROSOFT CORPORATION'S
REPLY IN SUPPORT OF ITS
MOTION TO DISMISS
CONSOLIDATED AMENDED
COMPLAINT

NOTE ON MOTION CALENDAR:
SEPTEMBER 8, 2023

ORAL ARGUMENT REQUESTED

TABLE OF CONTENTS

		Page
1		
2		
3	I. INTRODUCTION	1
4	II. ARGUMENT	2
5	A. Plaintiffs did not “communicate” with Zillow, which defeats all of	
6	Plaintiffs’ wiretapping claims.	2
7	B. Plaintiffs do not plead a Washington Privacy Act (“WPA”) claim.	4
8	C. Plaintiffs do not state a Missouri Wiretap Act (“MWA”) claim.	7
9	D. Plaintiffs do not state a California Invasion of Privacy Act (“CIPA”)	
10	claim.....	9
11	E. Plaintiffs’ Opposition confirms the rule of lenity should apply here.....	12
12	F. Plaintiffs do not state a claim for invasion of privacy.	14
13	1. Plaintiffs do not allege a reasonable expectation of privacy or	
14	“unreasonable” or “highly offensive” conduct by Microsoft.	14
15	2. Plaintiffs’ Washington and Illinois invasion of privacy claims fail	
16	for additional reasons.	17
17	III. CONCLUSION.....	17
18		
19		
20		
21		
22		
23		
24		
25		
26		

TABLE OF AUTHORITIES

Page(s)

CASES

<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	2
<i>Byars v. Goodyear Tire & Rubber Co.</i> , 2023 WL 1788553 (C.D. Cal. Feb. 3, 2023).....	10
<i>Commonwealth v. Spangler</i> , 809 A.2d 234 (Pa. 2002).....	8
<i>Cook v. Gamestop</i> , 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023).....	passim
<i>Cousineau v. Microsoft Corp.</i> , 992 F. Supp. 2d 1116 (W.D. Wash. 2012).....	4, 9
<i>Facebook, Inc. v. Duguid</i> , 141 S. Ct. 1163 (2021).....	4, 8, 13
<i>Fin. Software Sys. v. Questtrade, Inc.</i> , 2018 WL 3141329 (E.D. Pa. June 27, 2018).....	14
<i>Goldstein v. Costco Wholesale Corp.</i> , 559 F. Supp. 3d 1318 (S.D. Fla. 2021).....	3
<i>Gray v. Twitter Inc.</i> , 2021 WL 11086642 (W.D. Wash. Mar. 17, 2021).....	14
<i>Hammerling v. Google LLC</i> , 2022 WL 17365255 (N.D. Cal. Dec. 1, 2022).....	12
<i>Hazel v. Prudential Financial, Inc.</i> , 2023 WL 3933073 (N.D. Cal. June 9, 2023).....	12
<i>hiQ Labs v. LinkedIn Corp.</i> , 31 F.4th 1180 (9th Cir. 2022).....	13, 14
<i>In re Carrier IQ, Inc.</i> , 78 F. Supp. 3d 1051 (N.D. Cal. 2015).....	9
<i>In re Facebook, Inc. Internet Tracking Litigation</i> , 956 F.3d 589 (9th Cir. 2020).....	15

TABLE OF AUTHORITIES (continued)

Page(s)

<i>In re Google Inc. Cookie Placement Consumer Priv. Litig.</i> , 806 F.3d 125 (3d Cir. 2015).....	9, 15
<i>In re Meta Pixel Healthcare Litig.</i> , 2022 WL 17869218 (N.D. Cal. Dec. 22, 2022).....	9
<i>In re Nickelodeon Consumer Priv. Litig.</i> , 827 F.3d 262 (3d Cir. 2016).....	16, 17
<i>In re Vizio, Inc., Consumer Priv. Litig.</i> , 238 F. Supp. 3d 1204 (C.D. Cal. 2017)	12
<i>In re Zynga Priv. Litig.</i> , 750 F.3d 1098 (9th Cir. 2014)	10
<i>Jacome v. Spirit Airlines Inc.</i> , 2021 WL 3087860 (Fla. Cir. Ct. June 17, 2021)	3, 4
<i>Katz-Lacabe v. Oracle America, Inc.</i> , 2023 WL 2838118 (N.D. Cal. Apr. 6, 2023)	10
<i>Klumb v. Goan</i> , 884 F. Supp. 2d 644 (E.D. Tenn. 2012).....	9
<i>Luis v. Zang</i> , 833 F.3d 619 (6th Cir. 2016)	9, 12
<i>Phillips v. American Motorist Insurance</i> , 996 S.W.2d 584 (Mo. Ct. App. 1999).....	8, 9
<i>Popa v. Harriet Carter Gifts, Inc.</i> , 426 F. Supp. 3d 108 (W.D. Pa. 2019).....	2, 14
<i>Popa v. Harriet Carter Gifts, Inc.</i> , 52 F.4th 121 (3d Cir. 2022)	8
<i>Revitch v. New Moosejaw, LLC</i> , 2019 WL 5485330 (N.D. Cal. Oct. 23, 2021).....	3
<i>Rosenow v. Facebook, Inc.</i> , 2020 WL 1984062 (S.D. Cal. Apr. 27, 2020).....	12

TABLE OF AUTHORITIES (continued)

Page(s)

<i>Russo v. Microsoft</i> , 2021 WL 2688850 (N.D. Cal. June 30, 2021)	4
<i>Saber Interactive Inc. v. Oovee, LTD.</i> , 2022 WL 5247190 (W.D. Wash. Oct. 6, 2022)	11
<i>Saleh v. Nike, Inc.</i> , 562 F. Supp. 3d 503 (C.D. Cal. 2021)	3
<i>Samia v. Experian Info. Sols., LLC</i> , 2022 WL 298369 (S.D. Cal. Feb. 1, 2022)	7
<i>Schmidt v. Ameritech Ill.</i> , 768 N.E.2d 303 (Ill. App. Ct. 2002)	17
<i>Schuyleman v. Barnhart Crane & Rigging Co.</i> , 2023 WL 5427933 (W.D. Wash. Aug. 23, 2023)	6
<i>State v. Corliss</i> , 838 P.2d 1149 (Wash. Ct. App. 1992)	5, 6
<i>State v. Novick</i> , 384 P.3d 252 (Wash. Ct. App. 2016)	7
<i>State v. Roden</i> , 321 P.3d 1183 (Wash. 2014)	6
<i>Stokes v. Bally's Pacwest, Inc.</i> , 54 P.3d 161 (Wash. Ct. App. 2002)	7
<i>United States v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008)	15
<i>United States v. Hutchins</i> , 361 F. Supp. 3d 779 (E.D. Wis. 2019)	9
<i>United States v. Nosal</i> , 676 F.3d 854 (9th Cir. 2012)	1, 13
STATUTES	
18 U.S.C. § 2510(4)	8

TABLE OF AUTHORITIES (continued)**Page(s)**

18 U.S.C. § 2510(5)	9
18 U.S.C. § 2511	4
Cal. Penal Code § 631	10
Mo. Rev. Stat. § 542.400	7
Mo. Rev. Stat. § 542.402.2	9
Mo. Rev. Stat. § 542.408.4	8
RCW 9.73.030	4
RCW 9.73.060	4

RULES

Fed. R. Civ. Proc. 12(b)(6)	2
-----------------------------------	---

OTHER AUTHORITIES

Mark Huffner, <i>Is ‘session replay software’ a privacy threat or just improving your web experience</i> , Consumer Affairs (Oct. 25, 2022), https://www.consumeraffairs.com/news/is-session-replay-software-a-privacy-threat-or-just-improving-your-web-experience-102522.html	16
--	----

I. INTRODUCTION

In its Motion to Dismiss, Microsoft showed that Plaintiffs have not plausibly alleged they engaged in a “communication” when they interacted with Zillow’s website—which alone defeats their wiretapping claims. Additionally, as in *Cook v. Gamestop*, 2023 WL 5529772 (W.D. Pa. Aug. 28, 2023), *appealed filed*, No. 23-2574 (3d Cir. Aug. 29, 2023), which dismissed with prejudice wiretapping claims *based on the same Microsoft Clarity service as here*, Plaintiffs have not plausibly alleged their website actions contained the “contents” of any communication or were “private.” Importantly, Plaintiffs themselves embrace Zillow’s Terms of Use (TOU), which included its Privacy Policy that *disclosed* the technology at issue—so Plaintiffs, who are involved in other session replay cases, had no reasonable expectation that such technology *wasn’t* running on Zillow’s website.

Plaintiffs’ Opposition does not meaningfully respond to these arguments. Instead, Plaintiffs point back to their conclusory allegations that their website interactions were “communications,” Opp’n 12–13; continue to conclude that their mouse movements, clicks, and other website activity constitute “content,” even though under the weight of authority those are at best “record information” of the sort that “could have [been] obtained through a security camera at a brick-and-mortar store,” *Cook*, 2023 WL 5529772, at *8; and make no response to the fact that Clarity’s masking settings would have prevented Microsoft from accessing or collecting any text they input on Zillow’s website, *see* Compl. ¶ 64; MTD Ex. 2. Plaintiffs’ wiretapping claims should be dismissed for all these reasons, too.

Microsoft also showed that Plaintiffs’ wiretapping claims fail for the additional, independent reason that Plaintiffs are seeking to stretch criminal statutes beyond what is permitted under the rule of lenity, which would “unintentionally turn ordinary citizens into criminals.” *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012). Plaintiffs claim that the rule does not apply because there is no “grievous ambiguity” in the wiretapping statutes, but they never explain why “intercept,” “private,” “contents,” and “in transit” apply to the conduct here,

1 under the plain meaning of those terms. Instead, they admit that “session replay may not have
 2 been predictable when [the] Acts were passed.” Opp’n 28. The rule of lenity exists precisely to
 3 avoid the draconian outcome that Plaintiffs are pursuing.

4 Finally, as in *Cook*, which also dismissed with prejudice common law intrusion upon
 5 seclusion claims based on the Clarity service, and as in *Popa v. Harriet Carter Gifts, Inc.*, 426 F.
 6 Supp. 3d 108, 122 (W.D. Pa. 2019), which did so with respect to Plaintiff Popa’s claim as to a
 7 similar session replay service, Microsoft showed that Plaintiffs have not plausibly alleged a
 8 reasonable expectation of privacy or “unreasonable” or “highly offensive” conduct. In response,
 9 Plaintiffs point to highly generalized case law about privacy expectations and make a vague
 10 request for discovery. *See* Opp’n 29–32. But Plaintiffs nowhere explain how, as serial litigants
 11 visiting a website that disclosed its use of tracking technologies, Plaintiffs reasonably believed
 12 that Zillow would not use a third party’s diagnostic software to optimize its site. As in *Cook* and
 13 *Popa*, this Court should find that Plaintiffs do not meet the standard for a reasonable expectation
 14 of privacy or highly offensive conduct and should dismiss these claims, too.

15 Plaintiffs’ complaint suffers from the same “fundamental flaw” as in *Cook*: it fails to
 16 “plead the necessary facts to support [their] claims for violation of the [State] Wiretap Act[s] or
 17 intrusion upon seclusion.” *Cook*, 2023 WL 5529772, at *1. Rule 12(b)(6) demands dismissal.

18 II. ARGUMENT

19 A. Plaintiffs did not “communicate” with Zillow, which defeats all of Plaintiffs’ 20 wiretapping claims.

21 An undisputed threshold requirement of any State Wiretap Act claim is the presence of a
 22 “communication.” *See* MTD 8–10. As Microsoft showed and the Opposition confirms, Plaintiffs
 23 did not communicate with Zillow when they allegedly browsed Zillow’s website.

24 Plaintiffs argue they “clearly allege these were communications,” Opp’n 8, but simply
 25 saying so does not make it so. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (insufficient
 26 to merely parrot statutory language). Nor has Microsoft conflated “contents” with

1 “communications” as Plaintiffs contend. *See* MTD 21–24 (separately addressing the “content”
 2 issue). Rather, Microsoft makes the common sense argument that people do not ordinarily use or
 3 understand the term “communications” to describe browsing or filling out forms on internet
 4 websites, and there is no evidence the state legislatures intended to extend that term beyond its
 5 ordinary meaning. *See* MTD 8–10 (collecting cases).

6 Further, as Microsoft already showed (MTD 10 n.6), and as Plaintiffs concede (Opp’n 13
 7 n.1), the question whether the plaintiffs in *Saleh v. Nike, Inc.*, 562 F. Supp. 3d 503 (C.D. Cal.
 8 2021) had engaged in communications was not argued to the court. Nor was it adequately
 9 considered in *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2021).
 10 *Saleh* simply adopted without critique the plaintiffs’ framing of their website activity as
 11 “communications with Nike.” 562 F. Supp. 3d at 518. *Revitch* noted that a website user who
 12 clicks on “items of interest” on a website is akin to “a customer who calls to inquire about a
 13 store’s products.” 2019 WL 5485330, at *1. But that analysis, with which several courts,
 14 including the *Cook* court addressing the same Microsoft technology, have (rightly) disagreed—
 15 MTD 23–24 (discussing *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318 (S.D. Fla.
 16 2021) and *Jacome v. Spirit Airlines Inc.*, 2021 WL 3087860 (Fla. Cir. Ct. June 17, 2021)—is
 17 flawed because it wrongly analogizes a server’s automated response to a webpage query with
 18 actual verbal communication between humans.

19 Plaintiffs claim *Goldstein* and *Jacome*, which dismissed wiretapping claims involving
 20 session replay technology, actually support their position because those courts dismissed claims
 21 based on a “tracking device” exception to the definition of “electronic communications” in the
 22 Florida Security of Communications Act (“FSCA”). Plaintiffs claim this is proof that
 23 “communications” include “tracking.” Opp’n 12–13. But even a cursory read of *Goldstein* and
 24 *Jacome* confirm that those courts were extremely skeptical that the FSCA applied to website
 25 browsing behavior at all. *See Goldstein*, 559 F. Supp. 3d at 1321 (“[C]ontrary to Plaintiff’s
 26 interpretation, these [website] actions did not convey the substance of any communication.”);

1 *Jacome*, 2021 WL 3087860 at *3 (“[The legislatures] did not intend for [wiretapping law] to
 2 extend to the use of commonplace analytics software to improve a website browsers’ experience
 3”). The much simpler explanation for the FSCA’s “tracking device” exception is that the
 4 legislature took a “belt and suspenders approach in writing the statute” to ensure that law
 5 enforcement had access to necessary tools—not that the legislature intended to construe
 6 “communication” so broadly as to defy ordinary meaning. *See Facebook, Inc. v. Duguid*, 141 S.
 7 Ct. 1163, 1172 & n.7 (2021) (cleaned up) (rejecting similar argument).

8 Because Plaintiffs have not alleged facts showing their website interactions were
 9 “communications” under the Washington, Missouri, or California wiretapping laws, the Court
 10 should dismiss these claims with prejudice.

11 **B. Plaintiffs do not plead a Washington Privacy Act (“WPA”) claim.**

12 Plaintiffs’ WPA claim fails on multiple, additional grounds. *First*, the WPA’s
 13 wiretapping provision applies only to communications between “two or more *individuals*,” RCW
 14 9.73.030(1)(a), and not to Plaintiffs’ alleged one-way communications with Zillow. MTD 11.
 15 Plaintiffs do not identify any case law contradicting this clear holding in *Cousineau v. Microsoft*
 16 *Corp.*, 992 F. Supp. 2d 1116, 1129 (W.D. Wash. 2012). Instead, they attack an argument
 17 Microsoft didn’t make—that the WPA cannot apply to corporations *at all* because they are not
 18 “persons.” *See* Opp’n 15. Microsoft does not dispute that the WPA applies to corporate
 19 “persons” *if and when* they intercept a communication between “two or more individuals,” but
 20 that is not what Plaintiffs allege happened here. *Russo v. Microsoft*, 2021 WL 2688850, at *7
 21 (N.D. Cal. June 30, 2021), cited by Plaintiffs, analyzed the “person” language of
 22 Section 9.73.060—not the “two or more individuals” language of Section 9.73.030(1)(a). The
 23 non-WPA cases that Plaintiffs cite shed no light on the meaning of “individual” under the WPA
 24 because they discuss statutes that do not contain that limitation. *See* Opp’n 15; Cal. Penal Code
 25 § 631(a); 18 U.S.C. § 2511(1)(d).
 26

1 ***Second***, the WPA protects only “private” communications, and Plaintiffs have not
 2 plausibly alleged a reasonable expectation of privacy in using Zillow’s website. MTD 11–13. As
 3 explained by the *Cook* court when rejecting the plaintiff’s nearly-identical claims:

4 At most, the information that GameStop intercepted related to [Ms.
 5 Cook’s] product preferences. Product preference information is not
 6 personal information. This information is no different from what
 7 GameStop employees would have been able to observe if Ms. Cook
 8 had gone into a brick-and-mortar store and began browsing the
 9 inventory. Her physical movements in the store are like her mouse
 10 movements, her pauses to look at inventory are like her mouse
 11 pointer hovering over products, and her picking up video games off
 the shelf are like placing those same titles in her virtual cart. Ms.
 Cook certainly doesn’t have a reasonable expectation of privacy in
 this kind of public shopping behavior in the physical world, and she
 doesn’t have it in the digital world, either.

12 2023 WL 5529772, at *5. Identical reasoning applies here. Just as Plaintiffs cannot reasonably
 13 expect their presence at an open house is “private,” they cannot reasonably expect their browsing
 14 of a house *online* is “private.” This is especially true as to these Plaintiffs, who do not dispute
 15 being serial session replay litigants who have knowledge of the kinds of technologies that
 16 websites use. MTD 12. Finally, Plaintiffs embrace Zillow’s TOU, which incorporates Zillow’s
 17 Privacy Policy, and do not dispute that Zillow disclosed that it used session replay technology in
 18 that Policy.¹ *Compare id.*, with *generally*, Opp’n. The issue here is whether Plaintiffs reasonably
 19 could have expected “privacy” in their purported communications on a website that disclosed
 20 otherwise. *See State v. Corliss*, 838 P.2d 1149, 1151 (Wash. Ct. App. 1992), *aff’d*, 870 P.2d 317

23 ¹ The Court should deny Plaintiffs’ request to strike Zillow’s Privacy Policy because it is
 24 allegedly dated after Plaintiffs *first* visited the Zillow website. Opp’n 34–35. Plaintiffs link to the
 25 *current* Zillow TOU in their complaint, and so it is proper for Microsoft to attach the *current*
 26 Privacy Policy referenced in those terms. Compl. ¶ 18. And Plaintiffs allege they “routinely
 visit[]” Zillow’s website, *id.* ¶¶ 71–79, and do not deny that the Policy governs current use. The
 current Policy also links to earlier versions, which include substantially similar disclosures about
 tracking technology. *See, e.g.*, <https://www.zillowgroup.com/previous-privacy-policy/> (effective
 date January 1, 2020, addressing “Cookies, pixel tags, and other tracking technologies”).

(Wash. 1994);² *see also* Compl. 8 n.12 (citing Pew Research Center Survey that 79% of people know that websites collect online activities). They could not.

Third, Plaintiffs fail to allege that Microsoft “intercepted” any purported communications. *See* MTD 13–14. The Washington Supreme Court has held that to allege an interception, a plaintiff must show that the defendant “stop[ped] . . . before arrival . . . or interrupt[ed] the progress or course” of any communication or conversation. *Id.* (citing *State v. Roden*, 321 P.3d 1183, 1188 (Wash. 2014)). Plaintiffs plead only vague, conclusory allegations of interception of communications “between” Plaintiffs and Zillow, and “contemporaneously with their transmission,” Compl. ¶¶ 85, 124, 155, 186, 236, but their Opposition confirms they cannot point to any allegation showing that Microsoft collected their purported communications before Zillow, as *Roden* requires. *Compare also* Opp’n 17–18, with MTD 13–14 (collecting cases). Plaintiffs’ alternative response—that interception need not *prevent* receipt of the communication, Opp’n 18—is a straw man, since Microsoft never argued that.

Plaintiffs separately argue (Opp’n 17) they need not allege “interception” to state a WPA claim for “recording.” But Plaintiffs do not allege a WPA “recording” claim. *See* Compl. ¶¶ 122–24 (alleging violation of the *interception* prohibition), 118 (mentioning but not invoking the “recording” prohibition). A WPA recording claim is therefore not before the Court, and “[i]t is axiomatic that the complaint may not be amended by the briefs in opposition to a motion to dismiss.” *Schuyleman v. Barnhart Crane & Rigging Co.*, 2023 WL 5427933, at *3 (W.D. Wash. Aug. 23, 2023) (Robart, J.) (citation omitted).

Fourth, software is not a “device” under the WPA. *See* MTD 14. Plaintiffs’ authority does not hold otherwise. *See State v. Novick*, 384 P.3d 252, 254 (Wash. Ct. App. 2016) (cited at

² Plaintiffs attempt to neutralize the *Corliss* decision on the “privacy” element by noting that on appeal the Washington Supreme Court affirmed *Corliss* based on the lack of “interception” by a “device” without reaching whether a “private communication” was at issue. *See* Opp’n 17 n.2. But this hardly undermines the lower court’s ruling, i.e., that the defendant assumed the risk that a police informant would allow someone else to listen in to his phone call with the defendant. *See* MTD 13 (discussing *Corliss* in more detail).

1 Opp’n 18). There, the court did not hold that spying software was a “device”; it did not consider
2 the “device” element at all.

3 **Fifth**, Microsoft established that Plaintiffs consented to Zillow’s use of Clarity when they
4 continued using the Zillow website with notice of the Zillow TOUs that incorporate the Privacy
5 Policy. *See* MTD 13–15. Plaintiffs’ arguments around online contract formation are irrelevant, as
6 they admit they relied on (and thus agreed to) Zillow’s TOU. Comp. ¶¶ 113, 250. Since the
7 Privacy Policy is expressly incorporated into that agreement, they have therefore admittedly
8 accepted the Privacy Policy. *See Stokes v. Bally’s Pacwest, Inc.*, 54 P.3d 161, 164 (Wash. Ct.
9 App. 2002) (“[A] person who signs an agreement without reading it is generally bound by its
10 terms as long as there was ample opportunity to examine the contract and the person failed to do
11 so for personal reasons.”).

12 **Sixth**, Microsoft showed that Plaintiffs have not plausibly alleged that Microsoft’s
13 conduct caused each of them an injury to their business, person, or reputation. *See* MTD 15–16
14 (collecting cases). In response, Plaintiffs fail to identify any facts to support their conclusory
15 allegations of “mental anguish,” “emotional distress,” worry, fear, and “suffering arising from
16 their loss of privacy and confidentiality” Opp’n 19; Compl. ¶¶ 138–39. This does not suffice. *See*
17 MTD 15-16; *Samia v. Experian Info. Sols., LLC*, 2022 WL 298369, at *3 (S.D. Cal. Feb. 1,
18 2022) (dismissing claims following identity theft in part because plaintiff failed to plead facts to
19 support allegations that he “suffered emotional distress and damage to his credit worthiness”).

20 **C. Plaintiffs do not state a Missouri Wiretap Act (“MWA”) claim.**

21 Plaintiffs do not dispute that the MWA only prohibits interceptions of wire
22 communications involving “*aural* acquisition,” Mo. Rev. Stat. § 542.400(6); *see also* MTD 17.
23 Instead, they argue the word “aural” should be read *out* of the statute, primarily based on isolated
24 dicta from *Phillips v. American Motorist Insurance*, 996 S.W.2d 584 (Mo. Ct. App. 1999),
25 mentioning “e-mail” in a hypothetical. *Id.* at 591. But *Phillips* involved tapes of *phone*
26 *conversations*, not non-aural signals, so the court did not consider whether non-aural interactions

could somehow meet the MWA’s “aural acquisition” requirement. Nor does the fact the MWA was “mostly modeled” on the FWA make a difference, as Plaintiffs suggest. Opp’n 20. The FWA expressly prohibits the “aural *or other* acquisition” of the contents of a communication. 18 U.S.C. § 2510(4) (emphasis added). The MWA does not include the “other acquisition” language. Preemption does not save Plaintiffs’ claim, as the FWA only preempts state laws to the extent they afford less protection against wiretapping *by law enforcement*—not civil causes of action. *See Commonwealth v. Spangler*, 809 A.2d 234, 237 (Pa. 2002); *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125–26 (3d Cir. 2022).

Unable to satisfy the undisputed “wire communications” element of the MWA, Plaintiffs argue the spirit of *federal* law is “to evolve.” Opp’n 22. Even if true, that has no bearing on Missouri law, which prohibits only the interception of “wire communications” and does not extend to “electronic communications” like the FWA. *See* MTD 18–19. Plaintiffs ask the Court to infer otherwise by turning to the hypothetical of a wireless modem, but that is not the technology before the Court here and they cite no case law applying the MWA to “website communications” such as those alleged here, and Microsoft is aware of none. The Court should reject Plaintiffs’ invitation to effectively rewrite the MWA’s statutory language. *See Duguid*, 141 S. Ct. at 1172–73 (courts may not amend statutes even in the face of new technology).³

While Plaintiffs continue to insist that session replay software code is a “device,” they cannot identify a single Missouri court so holding and Microsoft is aware of none. This is unsurprising, as courts have regularly held otherwise under other wiretap laws. *See* MTD 17-18. Plaintiffs’ cases all involve different statutes with different language. *See United States v. Hutchins*, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) (interpreting the FWA as to the

³ Law enforcement’s obligation to indicate in their wiretap applications “whether the interception involves a cellular or other wireless device,” Opp’n 22 (citing Mo. Rev. Stat. § 542.408.4(2)) does not, as Plaintiffs suggest, change the plain language of the MWA. That administrative requirement likely accounts for the fact the FWA (unlike the MWA) protects cellular communications and, as already discussed, the FWA preempts less-protective state laws in the law enforcement context.

1 interception of “electronic communications,” which the MWA does not cover, and “Section
 2 2510(5)’s reference to ‘mechanism,’” also not in the MWA); *Luis v. Zang*, 833 F.3d 619, 634
 3 (6th Cir. 2016) (interpreting “device” under laws covering electronic communications).
 4 Plaintiffs’ other cases do not even discuss the “device” requirement. *See In re Meta Pixel*
 5 *Healthcare Litig.*, 2022 WL 17869218, at *12 (N.D. Cal. Dec. 22, 2022) (defendant did not raise
 6 whether advertising pixel qualified as a “device”); *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051,
 7 1084 (N.D. Cal. 2015) (not addressing whether software was a “device”); *Klumb v. Goan*, 884 F.
 8 Supp. 2d 644, 661 (E.D. Tenn. 2012) (never mentioning the word “device”).

9 Finally, it is undisputed that the MWA requires only the consent of *one party* to the
 10 conversation and Zillow (an alleged party) undisputedly consented to the use of Clarity.
 11 Plaintiffs claim the crime-tort exception applies because they say Zillow intercepted
 12 communications for the tortious purpose of violating the Missouri Merchandising Practice Act.
 13 *See* Opp’n 22–23 (citing Mo. Rev. Stat. § 542.402.2(3)); Compl. ¶¶ 255–62. Even if that were
 14 true (and it is not), it still would not revive Plaintiffs’ MWA claim against *Microsoft*. As several
 15 courts have clarified, the only the purpose that matters for this exception is that of the alleged
 16 interceptor. *See Phillips*, 996 S.W.2d at 589 (“It is not unlawful for a person to intercept a
 17 communication . . . or where one of the parties to the conversation has consented to the
 18 interception, *provided that he is not doing so for a ‘criminal or tortious’ purpose.*”) (emphasis
 19 added); *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 144–45, 145
 20 n.81 (3d Cir. 2015) (framing analogous inquiry under FWA as whether “the defendant . . . [has]
 21 the intent to use the illicit recording to commit a tort or crime”). Plaintiffs do not (and cannot)
 22 allege a criminal or tortious purpose by Microsoft, so Zillow’s consent defeats their MWA
 23 claims against Microsoft.

24 **D. Plaintiffs do not state a California Invasion of Privacy Act (“CIPA”) claim.**

25 Plaintiffs concede they do not allege claims under the first clause of Section 631,
 26 requiring dismissal of any such claim. *See* Opp’n 23. Their remaining CIPA claims fail because

1 they have not adequately alleged any of their website interactions constituted the “contents” of a
 2 communication. Cal. Penal Code § 631(a). Numerous courts have held that names, addresses,
 3 URLs, and information about how someone used a website—the things Plaintiffs allege
 4 Microsoft collected—are record information, not “contents” under CIPA. *See* MTD 21–24
 5 (collecting cases). Likewise, the court in *Cook* held that “none” of the “mouse movements and
 6 clicks, keystrokes, and URLs of web pages visited” allegedly collected by Microsoft’s Clarity
 7 service “constitutes the ‘content’ of ‘communications.’” 2023 WL 5529772 at *8 (citation
 8 omitted).

9 Seeking to side-step these cases, Plaintiffs respond that record information (such as a
 10 name) transforms into the content of a communication when typed into a web form. Opp’n 23–
 11 24. But their own authority shows otherwise. For example, in *Byars v. Goodyear Tire & Rubber*
 12 *Co.*, 2023 WL 1788553 (C.D. Cal. Feb. 3, 2023), the court held that a live online conversation
 13 with a Goodyear representative constituted the contents of communications because such a
 14 conversation “plausibly contain[ed] *more* than mere record [name and address] information.” *Id.*
 15 at *4 (emphasis added). And in *Katz-Lacabe v. Oracle America, Inc.*, 2023 WL 2838118 (N.D.
 16 Cal. Apr. 6, 2023), plaintiffs alleged they input text describing personal medical information into
 17 online forms, which the court held was “just barely enough” to plead content under CIPA. *Id.* at
 18 *9 (emphasis omitted). Unlike the plaintiffs in those cases, Plaintiffs here allege they input
 19 names, address, birth dates, phone numbers, and credit card numbers, which are all well-
 20 recognized categories of non-content “record” information, into text fields on the Zillow website.
 21 *See* Compl. ¶¶ 71–78; MTD App. A; MTD 22 (collecting cases). Plaintiffs do not describe any
 22 website interaction they had with Zillow that contained the “intended message conveyed by [a]
 23 communication” (i.e., contents), *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014),
 24 and their position that merely typing into webforms transforms record information into content
 25 “impermissibly render[s] the distinction between content and non-content in the statute
 26 superfluous.” *Cook*, 2023 WL 5529772, at *9.

1 Additionally, Plaintiffs do not plausibly allege Microsoft collected any webform
 2 information at all. *See* MTD 23–24. The complaint establishes that Clarity includes default
 3 masking settings that prevent Microsoft and its customers from collecting data typed into
 4 webforms, *see* Compl. ¶ 64; MTD Ex. 2, including the credit score, loan, and “other financial
 5 information” vaguely described by some (but not all) Plaintiffs, *see* MTD App. A. Plaintiffs do
 6 not allege Zillow changed these default settings, or had any reason to, so they have not met their
 7 burden to plausibly allege that Microsoft or Zillow possesses any alleged “contents.” *See Cook*,
 8 2023 WL 5529772, at *7 (dismissing complaint where plaintiff did not allege that GameStop had
 9 changed Clarity’s default masking setting or had “in fact, harnessed the capabilities [of Clarity],
 10 and it had the result of capturing the contents of specific communications”); *see also Saber*
 11 *Interactive Inc. v. Oovee, LTD.*, 2022 WL 5247190, at *8 (W.D. Wash. Oct. 6, 2022) (dismissing
 12 claims where plaintiff “pleaded no facts to create a ‘reasonable inference’ that the identified
 13 features are nonfunctional”). Plaintiffs cannot simply brush aside their own allegations about
 14 Clarity’s masking practices by now claiming masking raises a fact question.

15 Even if Plaintiffs had alleged communications (and they have not), their claim would still
 16 fail because they do not plausibly allege that Microsoft acted “intentional[ly]” or “willful[ly]” to
 17 intercept their communications. Again, the complaint establishes Microsoft uses default masking
 18 to *prevent* collection of text inputs on webforms. Compl. ¶ 64; MTD Ex. 2. Plaintiffs do not
 19 dispute that Microsoft prohibits use of Clarity “in connection with content which may contain
 20 sensitive user materials, such as . . . financial services” and requires its customers to comply with
 21 all privacy laws. *See* MTD Ex. 1 § 1(b)(ii), (iii); MTD 24–25. Thus, even if Plaintiffs had
 22 plausibly alleged they provided any such information to the Zillow website (and they have not),
 23 that still would not state a claim against Microsoft given the masking procedures and contractual
 24 requirements imposed by Microsoft on Zillow—defeating any “intentional” or “willful”
 25 argument as to Microsoft. Plaintiffs say a defendant need not intend to violate the law to be
 26 found liable, but that ignores that California courts interpret the term “willful” under CIPA to

mean that the defendant *knew* the communications were confidential—something Plaintiffs have not, and cannot, allege here. *See* MTD 24–25 (collecting cases).

Plaintiffs similarly fail to meaningfully respond to Microsoft’s showing they failed to sufficiently allege facts supporting interception “in transit.” *See* MTD 25–26 (discussing *Hammerling v. Google LLC*, 2022 WL 17365255 (N.D. Cal. Dec. 1, 2022); *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204 (C.D. Cal. 2017); *Rosenow v. Facebook, Inc.*, 2020 WL 1984062 (S.D. Cal. Apr. 27, 2020)). For one, they do not address or distinguish any of the relevant cases.⁴ Opp’n 25–26. And the cases on which they do rely do not apply, as one involved a genuine factual dispute on summary judgment regarding a highly technical patent, *Hazel v. Prudential Financial, Inc.*, 2023 WL 3933073, at *2 (N.D. Cal. June 9, 2023), and the other provided detailed allegations in the complaint about how the technology intercepted emails “as the communications are sent,” *Luis*, 833 F.3d at 630–31. Plaintiffs point to allegations that “wiretapping by Microsoft Clarity was ongoing for the duration of their visits” and that it took only 30 milliseconds “to send the captured Website Communications to Microsoft.” Opp’n 26. But they do not explain—and it is hardly evident—how either allegation plausibly supports their conclusion that Microsoft intercepted communications while in transit. Allegations of “potential capabilities” are insufficient. *Cook*, 2023 WL 5529772, at *7.

E. Plaintiffs’ Opposition confirms the rule of lenity should apply here.

Plaintiffs do not deny that each State Wiretap Act alleged is a criminal statute containing civil remedies. Because it is, at a *minimum*, ambiguous whether the terms “communications,” “intercept,” “private,” and “contents” extend to session replay software, the rule of lenity bars Plaintiffs’ State Wiretap Act claims against Microsoft. *See* MTD 26–29; *see also Cook*, 2023 WL 5529772, at *8 (observing that mouse movements and clicks have not “historically not been recognized as content” under wiretapping law; and considering them to naturally be “the cyber analog to record information” that could be observed by a security camera in a physical store).

⁴ Plaintiffs only discuss *Hammerling* with respect to their invasion of privacy claim.

As Plaintiffs themselves allege, session replay software is ubiquitous and not previously understood to constitute an unlawful wiretap. *See* Compl. ¶¶ 27–31. To now hold this commonplace software amounts to unlawful interception of private communications would “unintentionally turn ordinary citizens into criminals.” *Nosal*, 676 F.3d at 863.

Plaintiffs argue the State Wiretap Acts apply to session replay technology because the legislative histories and statutory texts suggest a broad intention “to protect historical privacy rights.” Opp’n 27–28. But the Ninth Circuit rejected that exact argument in *hiQ Labs v. LinkedIn Corp.*, 31 F.4th 1180 (9th Cir. 2022). There, and contrary to Plaintiffs’ contention that the court failed to consider “applying a criminal law civilly to emergent technologies,” Opp’n 28, the court considered whether “scraping” data from LinkedIn’s website in violation of a cease-and-desist letter was “without authorization” under the Computer Fraud and Abuse Act (“CFAA”). It answered “no” and applied the rule of lenity to the term “without authorization” “so as not to turn a criminal hacking statute into a ‘sweeping Internet-policing mandate.’” *hiQ Labs*, 31 F.4th at 1200–01. Importantly, the court so held *even though* the broad statutory purpose of the CFAA was to prevent digital trespass. *Id.* The Court should apply the same rationale here, where the Wiretap Acts language is at least as ambiguous as “without authorization” under the CFAA.

Nor may courts inject new meaning into old statutes to keep up with changing technology, as Plaintiffs suggest. In the Supreme Court’s words: “Court[s] must interpret what Congress wrote.” *Duguid*, 141 S. Ct. at 1172–73 (rejecting plaintiffs’ argument because the touchstone of statutory interpretation is the plain meaning, not the broad legislative purpose; and refusing to interpret robocall prohibition to reach new technologies not prohibited by the statute’s plain language, even though the statute’s underlying purpose was to prevent nuisance calls).⁵

⁵ Plaintiffs misconstrue an out-of-district case on personal jurisdiction and virtual contacts in urging this Court to reimagine the State Wiretap Acts. *See* Opp’n 28–29 (citing *Fin. Software Sys. v. Questrade, Inc.*, 2018 WL 3141329, at *5 (E.D. Pa. June 27, 2018)).

1 Plaintiffs wholly ignore *Gray v. Twitter Inc.*, 2021 WL 11086642 (W.D. Wash. Mar. 17,
 2 2021). But *Gray*, like *hiQ Labs*, underscores how common terms are at least ambiguous in the
 3 context of evolving technology—there, whether the term “telephone record” encompasses a
 4 “telephone number.” *Id.* at *9. Similarly, the average person would not understand session replay
 5 technology as amounting to wiretapping. Yet “[w]hen statutes have criminal consequences, the
 6 average person must be able to read the statute and understand what is, and what is not,
 7 prohibited.” *Id.* (citations omitted). The rule of lenity applies, and the Court should dismiss
 8 Plaintiffs’ wiretapping claims on this basis, too.

9 **F. Plaintiffs do not state a claim for invasion of privacy.**

10 Plaintiffs have not pleaded facts sufficient to state their primary (Washington) or
 11 alternative (Illinois and Missouri) claims for common law intrusion upon seclusion against
 12 Microsoft.⁶ These claims require both (1) a reasonable expectation of privacy, and
 13 (2) unreasonable or highly offensive conduct—both of which are lacking here. Nor do Plaintiffs
 14 dispute (or acknowledge) that a federal court already dismissed an invasion of privacy claim by
 15 Plaintiff Ashley Popa related to similar technology, *Popa*, 426 F. Supp. 3d at 122–23, and that
 16 the *Cook* court recently rejected the same claims involving the same Clarity service at issue here,
 17 2023 WL 5529772, at *10.

18 **1. Plaintiffs do not allege a reasonable expectation of privacy or “unreasonable”**
 19 **or “highly offensive” conduct by Microsoft.**

20 Plaintiffs cannot satisfy the first element of any of their common-law privacy claims—a
 21 reasonable expectation of privacy—for multiple, overlapping reasons:

- 22 • As the *Cook* court already held with respect to Clarity’s alleged use on
 23 Gamestop’s website, mouse clicks, browsing behavior, and name, address,
 24 financial, and other types of data input into texts fields on a website are not
 25 private facts as a matter of law, 2023 WL 5529772, at *10; *see also supra* 7–8;

26 ⁶ Plaintiffs do not bring a Pennsylvania common law claim against Microsoft. *Compare*
 Opp’n 29, with Compl. ¶¶ 159–72.

- 1 • Plaintiffs admit Clarity has default masking settings, and do not deny that these
- 2 settings would have prevented Microsoft from collecting information Plaintiffs
- 3 entered into text fields, *see* Compl. ¶ 64; MTD Ex. 2. As in *Cook*, where Clarity
- 4 masking processes were described in the complaint in the same manner and detail
- 5 as here, the masking processes establish that Clarity did not “in fact ... harness[]
- 6 the capabilities” described in Plaintiffs’ complaint. 2023 WL 5529772, at *7.
- 7 • Plaintiffs do not dispute that Zillow discloses its use of “tracking technologies” in
- 8 *both* its current and historical privacy policies, *see supra* note 1;
- 9 • Plaintiffs cannot deny that they are serial litigants with knowledge about how
- 10 session replay technology works, *see* MTD App. B (table of prior lawsuits); and
- 11 • Plaintiffs affirmatively allege that most consumers are aware that information
- 12 about their online activities is collected. *See* Compl. ¶ 31; *id.* 8 n.12 (citing 2019
- 13 Pew Research Center survey).

14 These alleged and/or admitted facts negate any reasonable expectation of privacy here.

15 Plaintiffs’ cases do not lead to a different outcome. Opp’n 30–32. Unlike in *In re Facebook, Inc.*

16 *Internet Tracking Litigation*, 956 F.3d 589, 601–02 (9th Cir. 2020), Plaintiffs point to nothing in

17 the Zillow TOU or Privacy Policy that led them to believe Zillow’s website would not use third-

18 party tracking technologies. Nor do Plaintiffs allege they took action to block Zillow from

19 collecting data from them. *See In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806

20 F.3d at 151 (reasonable expectation of privacy where plaintiffs activated a cookie blocker).

21 Instead, Plaintiffs’ allegations show they were aware Zillow used tracking technologies like

22 Clarity because they know such technologies are common-place and they acknowledge the

23 Zillow TOUs, which incorporate the Privacy Policy expressly disclosing this practice. Plaintiffs’

24 other cases are inapposite. *See United States v. Forrester*, 512 F.3d 500, 510 & n.6 (9th Cir.

25 2008) (addressing constitutional state action by law enforcement, not civil conduct).

26

1 **Second**, Plaintiffs neither allege facts showing “unreasonable” or “highly offensive”
 2 conduct by Microsoft, nor distinguish Microsoft’s cases. *See* MTD 31–33 (collecting cases).
 3 Plaintiffs do not dispute that Microsoft’s default masking policy prevents the collection of user-
 4 input text. *See* Compl. ¶ 64; MTD Ex. 2. And they do not deny that Microsoft requires customers
 5 to comply with all privacy laws and prohibits websites from using Clarity to collect sensitive
 6 data such as financial data. *See* MTD 29–32; Ex. 1 § 1(b)(ii). Under those circumstances, even
 7 taking all Plaintiffs allegations as true,⁷ Microsoft’s conduct in providing Zillow a service to
 8 better understand customer engagement on Zillow’s website is hardly “highly offensive.”
 9 Plaintiffs do not cite a single remotely analogous case, and the most analogous case—*Cook*,
 10 involving the very same Microsoft technology—unequivocally held otherwise: “The information
 11 that GameStop allegedly intercepted does not clear this threshold.” 2023 WL 5529772, at *4
 12 (relating to “mouse movements, clicks, keystrokes . . . URLs of web pages visited, and/or other
 13 electronic communications in real-time”).

14 Plaintiffs’ own cases support Microsoft’s position here. *See* Opp’n 32–33. The Third
 15 Circuit affirmed dismissal of privacy claims against Google because third-party cookies were
 16 common and “can serve legitimate commercial purposes,” even when used to track the web
 17 activities of children. *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 294 (3d Cir. 2016).
 18 And while the *Nickelodeon* court allowed claims against Viacom to proceed, that was because
 19 Viacom, unlike here, affirmatively represented to parents that it *would not* collect children’s
 20 personal information, such that they may have “created an expectation of privacy on Viacom’s
 21 websites [and] encouraged parents to permit their children to browse those websites under false
 22 pretenses.” *Id.* at 295.

23 ⁷ Paragraph 48 of the complaint even references an article that describes session replay
 24 code as “likely fully legal[.]” Mark Huffner, *Is ‘session replay software’ a privacy threat or just*
 25 *improving your web experience*, Consumer Affairs (Oct. 25, 2022),
 26 <https://www.consumeraffairs.com/news/is-session-replay-software-a-privacy-threat-or-just-improving-your-web-experience-102522.html>. It explains, “session replay was mainly used for troubleshooting and diagnostics. It’s useful for finding chokepoints where users are getting stuck or confused.”

1 **2. Plaintiffs’ Washington and Illinois invasion of privacy claims fail for**
 2 **additional reasons.**

3 Washington law requires, but Plaintiffs have not alleged, that Microsoft was
 4 “substantially certain” it lacked the necessary permission to deploy Clarity on Zillow’s website.
 5 MTD 33. Plaintiffs do not dispute that Microsoft makes Clarity available to website owners who
 6 must comply with all laws when they use it. *See* MTD Ex. 1 § 1(b)(ii). On these facts, Plaintiffs
 7 cannot allege (and have not alleged) that Microsoft was “substantially certain” that it lacked
 8 necessary permission to provide session replay software to Zillow. MTD 25, 33. The detours in
 9 Plaintiffs’ Opposition into whether Zillow’s Privacy Policy was browswrapped or clickwrapped
 10 have no bearing on Microsoft’s certainty around lack of consent.

11 And as for their Illinois claim, Plaintiffs point to no factual allegations showing they
 12 suffered injury as a result of Microsoft’s conduct as Illinois law requires. *See* MTD 33–34. As
 13 explained, Plaintiffs’ assertions of mental anguish, emotional distress, and suffering are factually
 14 unsupported and implausible. *See supra* 9; MTD 16, 33–34. And any such distress would not
 15 have been caused by *Microsoft* here given its requirements surrounding use of Clarity; its
 16 masking procedures; and Zillow’s disclosure that it uses tracking technologies. And intrusion
 17 upon seclusion is not itself an injury under Illinois law. *See Schmidt v. Ameritech Ill.*, 768 N.E.2d
 18 303, 316 (Ill. App. Ct. 2002) (requiring “actual injury *in the form of*, for example, medical care,
 19 an inability to sleep or work, or a loss of reputation and integrity in the community”).

20 **III. CONCLUSION**

21 For the foregoing reasons and those in its Motion to Dismiss, Microsoft respectfully
 22 requests that the Court dismiss Plaintiffs’ complaint against it with prejudice.
 23
 24
 25
 26

1 DATED: September 8, 2023

2
3 I certify that this brief contains 5,987 words, in compliance with the Local Civil Rules
4 and this Court's Order of September 6, 2023.

5
6
7 By: /s/ Nicola C. Menaldo

8 Nicola C. Menaldo, Bar No. 44459
9 Anna Mouw Thompson, Bar No. 52418
10 **Perkins Coie LLP**
11 1201 Third Avenue, Suite 4900
12 Seattle, Washington 98101-3099
13 Telephone: +1.206.359.8000
14 Facsimile: +1.206.359.9000
15 NMenaldo@perkinscoie.com
16 AnnaThompson@perkinscoie.com

17 James G. Snell, Bar No. 173070
18 **Perkins Coie LLP**
19 3150 Porter Drive
20 Palo Alto, California 94304-1212
21 Telephone: +1.650.838.4300
22 Facsimile: +1.650.838.4350
23 JSnell@perkinscoie.com

24 *Attorneys for Defendant Microsoft Corporation*